Adoption of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware in OSG and EGEE

Overview

- OSG & EGEE Authorization Models
- Authorization Interoperability Profile
- Implementations and Deployments

CHEP 2010
Oct 19, 2010

Gabriele Garzoglio
Computing Division, Fermilab

The Collaboration

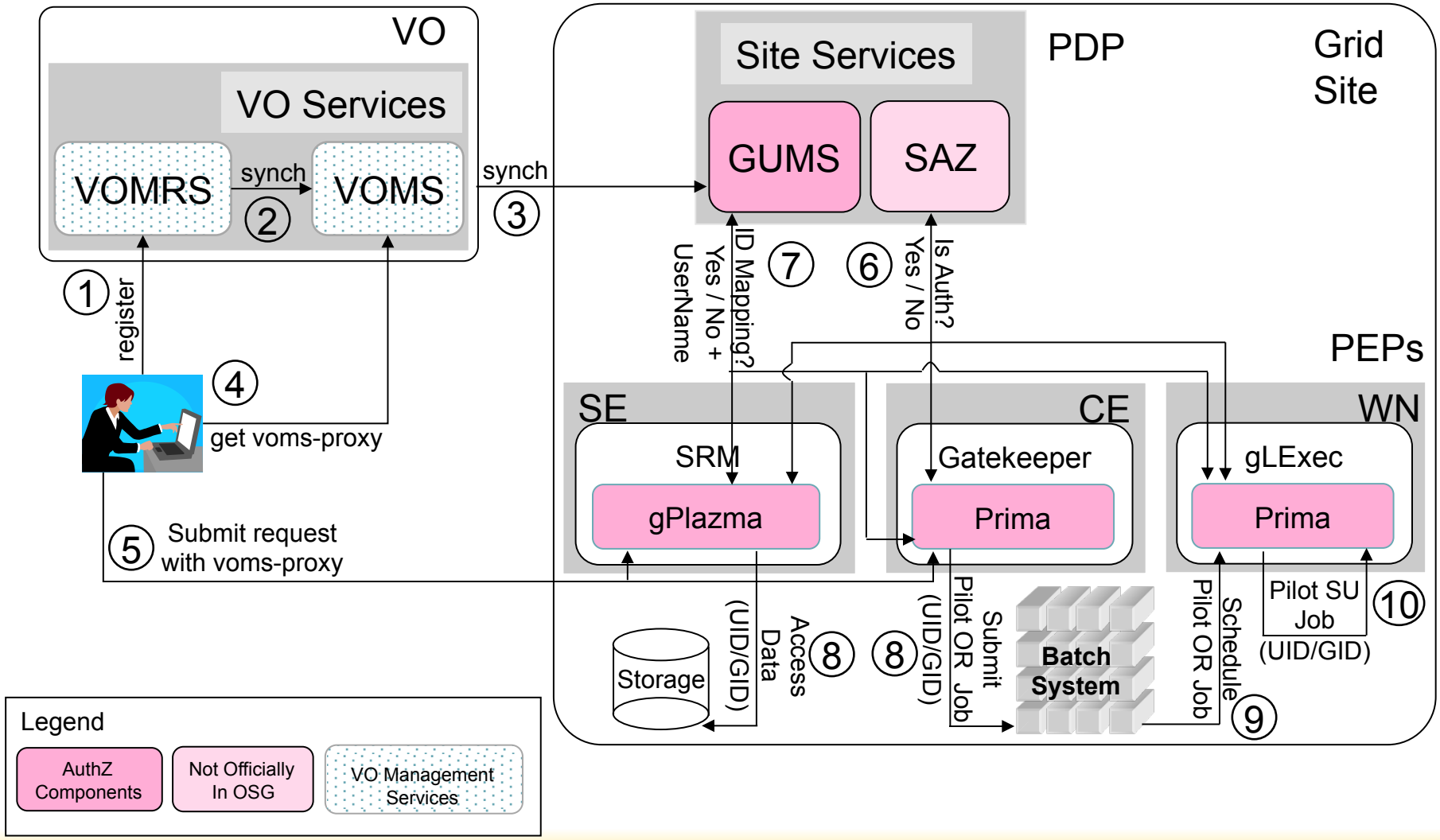
Ian Alderman[9]
Mine Altunay[1]
Rachana Ananthakrishnan[8]
Joe Bester[8]
Keith Chadwick[1]
Vincenzo Ciaschini[7]
Yuri Demchenko[4]
Andrea Ferraro[7]
Alberto Forti[7]
Gabriele Garzoglio[1]
David Groep[2]
Ted Hesselroth[1]
John Hover[3]
Oscar Koeroo[2]
Chad La Joie[5]
Tanya Levshina[1]
Zach Miller[9]
Jay Packard[3]
Håkon Sagehaug[6]
Valery Sergeev[1]
Igor Sfiligoi[1]
Neha Sharma[1]
Frank Siebenlist[8]
Valerio Venturi[7]
John Weigand[1]

[1] *Fermilab, Batavia, IL, USA*
[2] *NIKHEF, Amsterdam, The Netherlands*
[3] *Brookhaven National Laboratory, Upton, NY, USA*
[4] *University of Amsterdam, Amsterdam, The Netherlands*
[5] *SWITCH, Zürich, Switzerland*
[6] *BCCS, Bergen, Norway*
[7] *INFN CNAF, Bologna, Italy*
[8] *Argonne National Laboratory, Argonne, IL, USA*
[9] *University of Wisconsin, Madison, WI, USA*

The Authorization Model

- The EGEE (EGI) and OSG security model is based on **X509** end entity and proxy **certificates** for single sign-on and delegation
- Role-based access to resources is based on **VOMS Attribute Certificates**
- Users **push credentials** and **attributes** to resources
- Access **privileges** are granted with appropriate **local identity mappings**
- Resource gateways (Gatekeeper, SRM, gLExec, …) i.e. Policy Enforcement Points (**PEP**) **call-out** to site-central Policy Decision Points (**PDP**) for authorization decisions

Authorization Infrastructure (the OSG case)



Goals for Interoperability

- Agree on **common PEP to PDP call-out protocol** and **implementation** to…
  1. …share and reuse software developed for EGI and OSG
  2. …give software providers (external to the Grid organizations) reference protocols to integrate with both Grids infrastructures
  3. …enable the seamless deployment of software developed in the US or EU in the EU or US security infrastructures

AuthZ Interoperability Activities

- 2008
  - **Release XACML profile** document: result of 1+ yr collaboration between OSG, EGEE, Globus, and Condor.
  - **Implementation and integration** of XACML AuthZ modules with principal PDPs and PEPs in OSG and EGEE
  - Demonstrated interoperability of OSG vs. EGEE deployments in ad-hoc scenarios – **Goal 3**
- 2009
  - Discussion on evolutions of the profile in the context of Argus
  - **Argus extends** the interoperability **profile**
  - External software providers use the profile as reference on authorization for the Grid Domain. TechX: SVOPME project. Globus: GT5 – **Goal 2**
- 2010
  - Consolidation of **additional** OSG **PDPs** and **PEPs**
  - Start migration of PEPs to LCAS / LCMAS (Nikhef, NL) as common code base – **Goal 1**
- 2011
  - Additional migration of OSG sites to XACML

Adoption of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware in OSG and EGEE

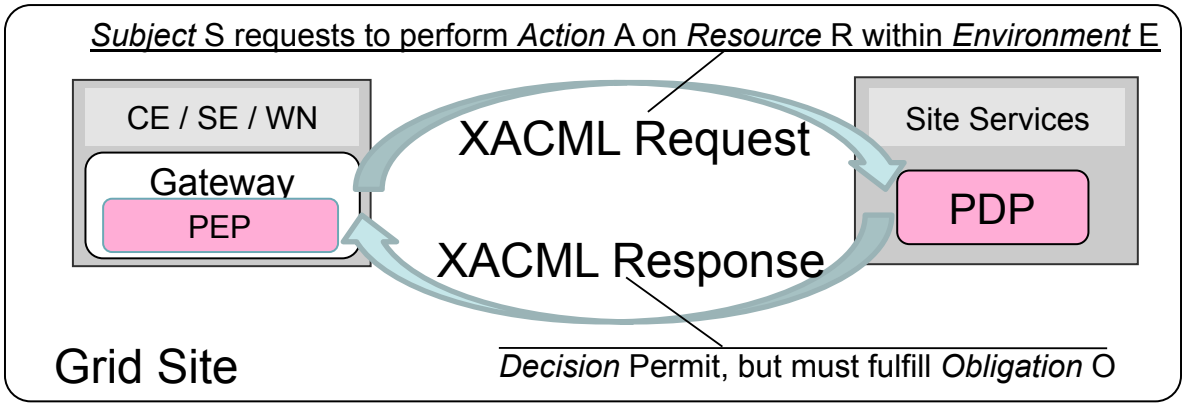
Overview

- ✓ OSG & EGEE Authorization Models
- ➢ Authorization Interoperability Profile
- • Implementations and Deployments

CHEP 2010
Oct 19, 2010

Gabriele Garzoglio
Computing Division, Fermilab

Request/Response Attribute Categories



- Request is made with
  - Subject attributes
  - Action attributes
  - Resource attributes
  - Environment attributes
- Response is made with
  - Permit, Deny, or Indeterminate
  - Obligation attributes

Request Attributes

- Subject (see profile doc for full list)
  - Subject-X509-id
    - String: OpenSSL DN notation
  - Subject-VO
    - String: “CMS”
  - VOMS-FQAN
    - String: “/CMS/VO-Admin”
- Resource (see doc for full list)
  - Resource-id (enum type)
    - CE / SE / WN
  - Resource X509 Service Certificate Subject
    - resource-x509-id
  - Host DNS Name
    - Dns-host-name
- Action
  - Action-id (enum type)
    - Queue / Execute-Now / Access (file)
  - Res. Spec. Lang.
    - RSL string
- Environment
  - PEP-PDP capability negot.
    - PEP sends to PDP supported Obligations
    - Enables upgrading of the PEPs and PDPs independently
  - Pilot Job context (pull-WMS)
    - Pilot job invoker identity
    - Policy statement example: “User access to the WN execution environment can be granted only if the pilot job belongs to the same VO as the user VO”

Obligation Attributes

- UIDGID
  - UID (integer): Unix User ID local to the PEP
  - GID (integer): Unix Group ID local to the PEP
- Secondary GIDs
  - GID (integer): Unix Group ID local to the PEP (Multi recurrence)
- Username
  - Username (string): Unix username or account name local to the PEP.
- Path restriction
  - RootPath (string): a sub-tree of the FS at the PEP
  - HomePath (string): path to user home area (relative to RootPath)
- Storage Priority
  - Priority (integer): priority to access storage resources.
- Access permissions
  - Access-Permissions (string): "read-only", "read-write"

Adoption of a SAML-XACML Profile for Authorization Interoperability across Grid Middleware in OSG and EGEE

Overview

- ✓ OSG & EGEE Authorization Models
- ✓ Authorization Interoperability Profile
- ➢ Implementations and Deployments

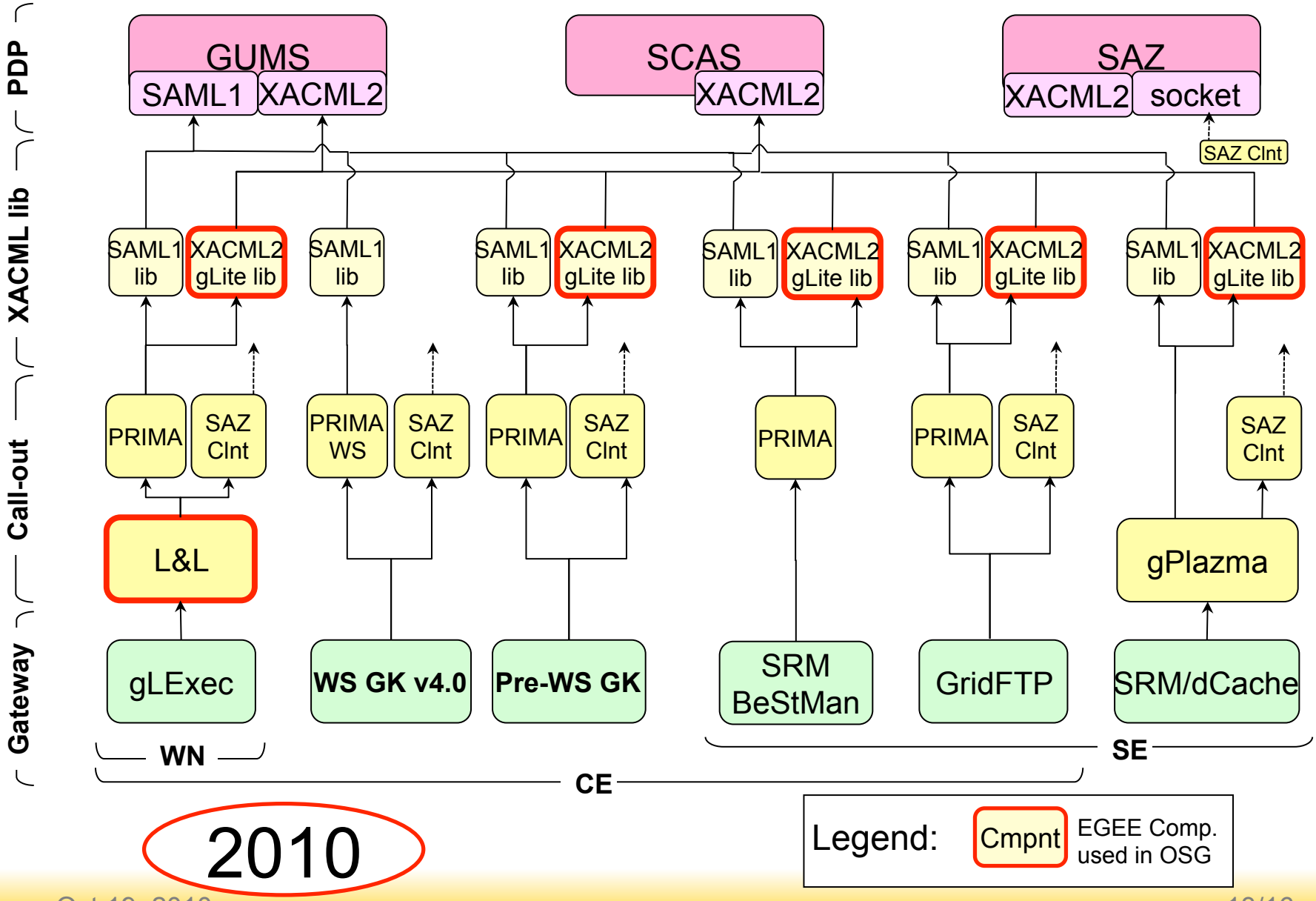
CHEP 2010
Oct 19, 2010

Gabriele Garzoglio
Computing Division, Fermilab

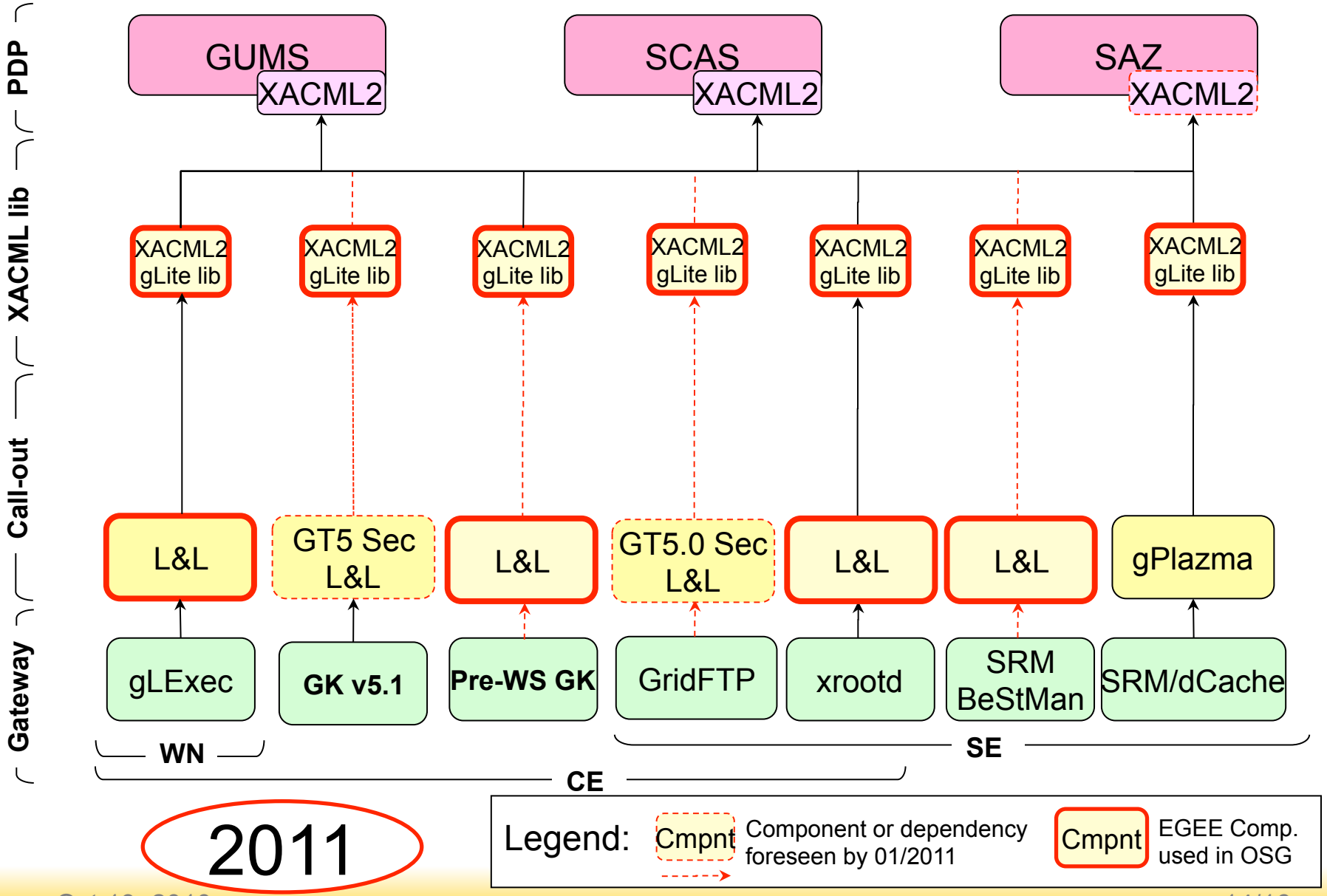
Implementations

- SAML v2 - XACML v2 profile
  - OpenSAML (Java); Globus XACML (C)
- Authorization Callout Modules and PDPs
  - LCAS / LCMAPS (L&L) - SCAS plug-in → SCAS (EGEE)
  - PRIMA - gPlazma plug-in → GUMS / SAZ (OSG)
- Resource Gateways
  - Computing Element
    - Pre-WS and WS Gatekeepers 4.2 (5.1 in progress)
  - Storage Element
    - SRM / dCache; BeStMan; xrootd; GridFTP
  - Worker Node
    - gLExec

XACML Callout Structure - using EGEE code in OSG



XACML Callout Structure - using EGEE code in OSG



Deployments

- Getting traction slowly: **migration requires** packaging and administrative **work to simplify** the infrastructure with **no new functionalities**
- UNL is now enabling access to Hadoop for all SE Grid interfaces (SRM/BeStMan, GridFTP, xrootd) via XACML.
  XACML-only access for SE, CE, and WN interfaces (Gatekeeper, gLExec) is being tested
- We are working closely with VDT to make the deployment of the new infrastructure easy.

Conclusions

- An EGEE, OSG, Globus, and Condor collaboration has released in 2008 an Authorization Interoperability profile and XACML implementation
- Call-out module implementations are integrated with major Resource Gateways
- The major advantages of the infrastructure are:
  1. share and reuse software developed for EGI and OSG
  2. give software providers reference protocols to integrate with both Grids infrastructures
  3. when using the same release of the protocol, enable the deployment of software developed in the US or EU in the EU or US security infrastructures
- Production deployments are slowly getting traction